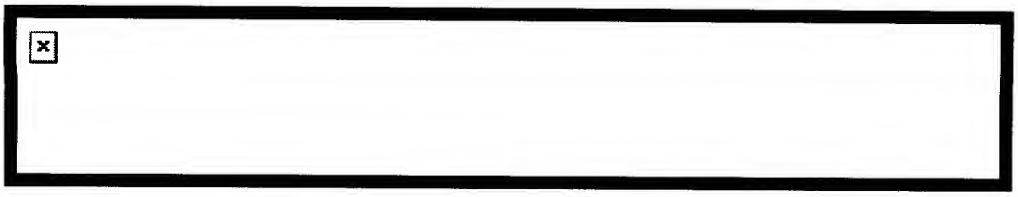

CREATING AN ELECTRONIC MONETARY SYSTEM

by Sholom Rosen

Citibank

The Electronic Monetary System (EMS) is a highly versatile and highly secure payment system that creates, secures, and exchanges electronic notes in multiple currencies. EMS is a serious attempt to build a comprehensive electronic money system that reflects the interests of the regulatory authorities, the banking system as it exists today, and the rapid manner in which technology will continue to change. The system is the first to support, in a secure fashion, electronic cash payments for both retail and wholesale customers.

Having worked to develop EMS since 1991, Citibank was awarded two important technology patents covering EMS and electronic money in 1995 by the U.S. Patent and Trademark Office. The bank also has several other patents pending in the area of electronic commerce.

The implications of electronic money in today's globally networked world are enormous. The steadily growing popularity of PCs, the Internet, online services, and electronic gadgets of every kind, means more and more individuals are benefiting from technology's push into the consumer world. Electronic money introduces an entirely new scheme for transacting business. Consumers and merchants will be able to perform fairly complicated financial transactions without having to go to a bank.

EMS involves four basic types of participants:

1. *Issuing banks* generate electronic notes (money) on demand to customers; there can be any number from one to many. 2. *Correspondent banks* accept and distribute the electronic money.

3. *Clearing banks* clear issuing bank notes and settle accounts.

4. *Subscribers* (buyers and sellers) use Money Modules (essentially a secure processing environment) for storing their electronic money, performing online transactions with a bank, or exchanging electronic money with other Money Modules.

EMS notes can be created on demand in any currency. The notes can be withdrawn as cash from a DDA (Demand Deposit Account) or used to draw down an approved line of credit. Each note carries a complete electronic audit trail and is reconciled by the issuing bank. EMS cash notes circulate and can be redeemed at the bank or transferred to another subscriber. And like cash, the value of each note is guaranteed by a bank.

With the potential for fraudulent use of electronic money systems, EMS was designed to include the three basic principles of security: prevention, detection, and containment. EMS addresses prevention through the use of cryptographic protocols and physical protection of the Money Modules. Each communications session is authenticated and secured, and a Security Server authenticates each Money Module by periodically validating its electronic certificate. A special protective coating makes the Money Module hardware itself tamperproof, thus physically protecting the sensitive software contained within it.

To aid in identifying duplicate or counterfeit notes, EMS (invisibly to the user) regularly "sweeps" electronic notes into the bank for validation and control, and then returns new notes to the Money Module. The system also reconciles notes cleared to notes issued. EMS "contains" suspected fraudulent use in several ways: First, electronic notes carry an expiration date which limits the window of opportunity for transfers. (This does not cause the value of the notes to expire--just the ability to move them.) EMS can also block both the further use of Money Modules that are known to be corrupted and the further circulation of fraudulent notes. The system can also cause a Money Module certificate to expire, thereby putting the Money Module out of commission.

EMS strikes a balance between the needs for security and privacy. The system addresses the twin issues of system security and customer privacy in a manner that guarantees the traceability of every transaction without knowing the identity of the customer. Protecting the customers' trust and system integrity are critical.

EMS provides an infrastructure for applications such as simple retail point-of-sale, electronic payments between corporations, interbank payments, and party-to-party foreign exchange.

The technology also extends well beyond moving money securely. Additional technology addresses and resolves the security and processing needs required for commerce over open networks. The slow growth of electronic commerce over "open" networks, such as the Internet, is due not only to the poor security across the network but also the absence of adequate protection for the buyer and seller as they attempt to conduct business without any face-to-face contact.

One basic risk of doing business over open networks, for example is that of "pulling the plug"--either the buyer can pull the plug upon receipt of the goods (but before paying) or the seller can pull the plug upon receipt of payment (but before shipping the goods). In cyberspace, the secure receipt of both payment and electronic goods must be redefined.

A companion technology known as Trusted Agent was designed along with EMS to guarantee payment and delivery for electronic goods and services purchased over the Internet or any open network. Through the use of secure transaction "umbrellas," EMS and Trusted Agent together can ensure that both the customer and the merchant are safe because payment and delivery are locked and synchronized. Payments will be released to the merchant, and the electronic goods released to the buyer, only upon the successful exchange of both sides of the transaction.

The combination of EMS and Trusted Agent for the first time enables truly open spontaneous electronic commerce because both the buyer and the seller are protected from the risks associated with not doing business face-to-face. Trusted Agent not only integrates information with the movement of money, but can verify that the cybermerchant is actually who it purports to be. Trusted Agent also carries information explaining the nature of a payment (such as an invoice number, which is required by businesses when posting payments), and creates and delivers a secure receipt at the end of a transaction.

Trusted Agent's ability to guarantee payment and delivery need not be restricted to electronic money applications. Trusted Agent in addition can deliver credit cards, or debit cards as the payment medium over an electronic network.

The versatility and security of the combination of EMS and Trusted Agent technologies can provide the needed functionality and trust of the physical marketplace to open networks.

Prepared for the Cato Institute's 14th Annual Monetary Conference, May 23, 1996, Washington, D.C.

BACK